UNITED STATES DISTRICT COURT

for the

Southern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

One (1) Samsung SM-N950U cellular Telephone
(further described in Attachment B)

Case No. M-19-1233-M

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment B

located in the Southern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment C

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ✔ evidence of a crime;
- ✔ contraband, fruits of crime, or other items illegally possessed;
- ✔ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 952	Illegal importation of a Schedule II controlled substance

The application is based on these facts:

See Attachment A

- ✔ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

approved by: M. Alexis Garcia
5/29/19

Applicant's signature

Jorge Rodriguez, HSI Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: May 30, 2019

Judge's signature

City and state: McAllen, Texas

Hon. Peter E. Ormsby, United States Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT
COURT FOR THE SOUTHERN DISTRICT
OF TEXAS MCALLEN DIVISION

IN THE MATTER OF THE SEARCH OF ONE SAMSUNG SM-N950U CELLULAR TELEPHONE LISTED IN ATTACHMENT B, CURRENTLY LOCATED AT 5901 S. INTERNATIONAL PARKWAY; MCALLEN, TEXAS 78503	Case No. M-19-1233-M

ATTACHMENT A

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Jorge Rodriguez, a Task Force Officer with the Homeland Security Investigation, being duly sworn, hereby depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—one electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. Your Affiant is a Task Force Officer with Homeland Security Investigations (HSI) assigned to the Office of the Assistant Special Agent in Charge (ASAC) in McAllen, Texas, has been a sworn Law Enforcement officer since April 2007, when he began his career at the United States Customs and Border Protection, Hidalgo Port of Entry. Affiant served as a Customs and Border Protection Officer, where he served as an Officer and Supervisor. The affiant completed a twelve (12) week training academy at the Federal Law Enforcement Training Center

(FLETC) in Brunswick, Georgia. The affiant was assigned to the Office of the Assistant Special Agent in Charge (ASAC) in McAllen, Texas in 2017 and has served as a Task Force Officer. As a Task Force Officer with Homeland Security Investigations, the affiant is a sworn federal law enforcement officer with the authority to investigate federal offenses pursuant to Title 8, Title 18, Title 19 and Title 21 of the United States Code, amongst others. The affiant is currently assigned to a Drug Smuggling investigations group that investigates controlled substances trafficking and smuggling offenses committed by controlled substances trafficking organizations. The affiant has since received numerous additional Law Enforcement trainings from the Department of Homeland Security as well as various other federal, state and local accredited institutions. Affiant has conducted numerous investigations resulting in the arrest and successful prosecution of misdemeanor and felony cases at the federal level. Through these investigations, the affiant has conducted numerous hours of surveillance, interviews, debriefs, executed numerous search warrants, and seized numerous controlled substances.

3. The information in this affidavit is based on my personal knowledge and information provide to me by other law enforcement officers and individuals. The information in this affidavit is provided for the limited purpose of establishing probable cause. The information is not a complete statement of all the facts related to this case.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a Samsung cellular telephone, Model SM-N950U, IMEI: 358505083517553, S/N: R28J947G9NX, hereafter referred to as "electronic device 1." This electronic device is currently in secure evidence storage at the HSI McAllen office located at 5901 S. International Parkway; McAllen, Texas 78503.

5. The applied-for warrant would authorize the forensic examination of the electronic device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On May 15, 2019, at approximately 5:58pm, a red 2018 Peterbilt Tractor bearing Texas license plate number R298136 (hereafter referred to as Load Vehicle) pulling a Lufkin trailer was encountered at the United States Border Patrol Checkpoint on US Highway 281 North near Falfurrias, Texas. Hortencia LERMA, (hereafter referred to as LERMA) was the driver and sole occupant of the Load Vehicle. During the immigration inspection, the Border Patrol Agent observed LERMA exhibiting nervous behavior and LERMA's hands shaking. The Load Vehicle was subsequently sent to secondary inspection.

7. In secondary inspection, a Border Patrol Agent asked LERMA for consent to search the Load Vehicle, which LERMA granted. A canine inspection was conducted by a trained and certified canine team, which resulted in the positive alert to the odor of controlled substance(s) emanating from the Load Vehicle.

8. A physical search of the Load Vehicle revealed a total of eight (8) cellophane wrapped packages concealed within a closet behind the passenger's seat of the Load Vehicle. The packages contained a white powdery substance which field tested presumptive positive for the properties and characteristics of cocaine. The total weight of the cocaine was approximately 8.82 kilograms (kg) on a calibrated scale.

9. LERMA declined to be interviewed by HSI agents.

10. LERMA was arrested and charged with violations of 21 U.S.C. § 841, possession with intent to distribute a controlled substance and 21 U.S.C. § 846, conspiracy to possess with intent to distribute a controlled substance.

11. LERMA had one cellular telephone in her possession, a Samsung SM-N950U, which was seized. LERMA's cellular telephone is "electronic device 1," the subject of this search warrant.

12. Cellular telephones have become an integral part of daily living. Persons with cellular telephones utilize them for communicating with others, taking and storing photographs and videos, mapping and direction seeking, online purchasing and to maintain many records that have historically been kept on paper. A person's cellular telephone use will often reflect crimes they are involved in, such as: motives, purchases of implements utilized in a crime, communication through electronic mail or text messaging involving the crime or coconspirators, pictures of contraband, and travel plans indicative of flight to avoid prosecution.

13. Conducting a search of a cellular telephone, documenting the search, and making evidentiary and discovery copies is a lengthy process. It is necessary to determine that no security devices are in place which could cause the destruction of evidence during the search; in some cases, it is impossible even to conduct the search without additional expert technical assistance. Since digital evidence is extremely vulnerable to tampering or to destruction through error, electrical outages, and other causes, removal of the system from the premises where seized was necessary to retrieve the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. It would have been extremely difficult to secure the system on the premises during the entire period of the search; this process might easily take days or weeks.

A qualified local, state, or federal law enforcement officer will utilize specialized training and equipment to obtain the contents of digital evidence contained within the cellular telephone, where normal methods are not successful.

14. Your affiant knows that drug smuggling is often a conspiratorial crime. Through his training and experience, your affiant knows that individuals often take pictures, videos, send text messages, and other uses of digital media which will implicate or document the crimes in which they take part. Additionally, a search of the contact list, call logs, text messages and other digital media contained within the cellular telephones is likely to identify additional conspirators in the crimes. It is likely that the electronic device contains electronic records relating to the offenses and information that can lead to the identification of co-conspirators and locations of travel.

15. The aforementioned electronic device is currently in the lawful possession of HSI, and in secured evidence storage.

16. Your affiant hereby requests a search warrant for a search of the electronic device named herein and further described in Attachment B, and its contents therein, for evidence of the crimes of violations of Title 21 United States Code Section 841 and 846 regarding the possession with intent to distribute a controlled substance and conspiracy to possess with intent to distribute a controlled substance, specifically photographs, images, depictions, text messaging, contact lists, call logs, email, or any other material involved in unlawful activities detailed above. Your affiant requests a search for records, documents, and materials that constitute proof of said crimes and search said electronic device for images or material relating to the above crimes and documents or files evidencing the source or origin thereof, along with any indicia of use, ownership, dominion, or control over the electronic device to be searched including receipts, payments, bills,

correspondence, account subscriber information, documents or files declaring identity or source of authorship, photographs of any persons involved in the criminal conduct, and all of the above records, together with any evidence or items which would be used to conceal the forgoing or prevent its discovery. In the search requested herein, the volume of digital information for law enforcement to search may be significant, which would result in a process that requires days and possible weeks. Finally, your affiant requests that the Court authorize the assistance of a duly qualified law enforcement officer or qualified technician acting under the direction of authorized law enforcement to execute the forensic examination of the cellular telephone for the amount of time needed to complete the examination.

13. Based on the aforementioned factual information, your affiant respectfully submits that there is probable cause that all images, photographs and videos; any numeric, text and voice messages; stored names and phone numbers; GPS information contained in the memory function information requested in this Search Warrant Affidavit and Application will be found in the electronic device further described in Attachment B to be searched and will constitute evidence of the violations of Title 21 United States Code Section 841 and 846 regarding the possession with intent to distribute a controlled substance and conspiracy to possess with intent to distribute a controlled substance, and I respectfully request that the search warrant be issued.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images.

Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

b. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

c. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive

e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

d. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "Wi-Fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

e. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g.,

121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

i. Removable data storage devices or media are used for storing data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Removable data storage devices or media can store word-processing documents, spreadsheets, presentations, photographic images, video recordings, GPS information, and any other digital media or documentation.

15. Based on my training, experience, and research I know that the removable data storage devices have capabilities that allow them utilize internet, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed and/or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. There is probable cause to believe that things that were once stored on the device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in

particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

18. *Forensic evidence.* As further described in Attachment C, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

e. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such

as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

f. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

g. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

h. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

i. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

19. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

20. *Manner of execution.* Because this warrant seeks only permission to examine device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

21. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the electronic device described in Attachment B to seek the items described in Attachment C. I respectfully request the issuance of this search warrant and that all evidence be seized and held for future court action.

Respectfully submitted,

Jorge Rodriguez
Task Force Officer
Homeland Security Investigations

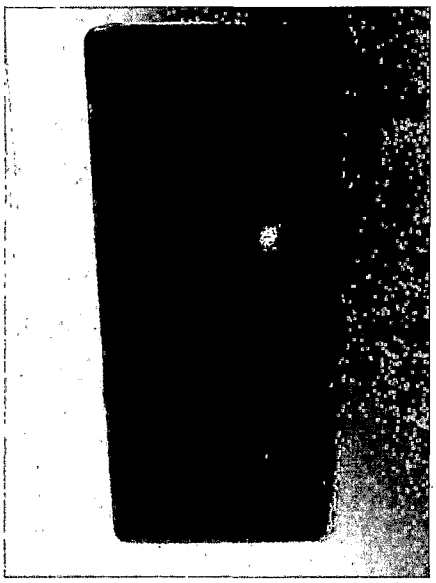
Subscribed and sworn to before me on May 30, 2019

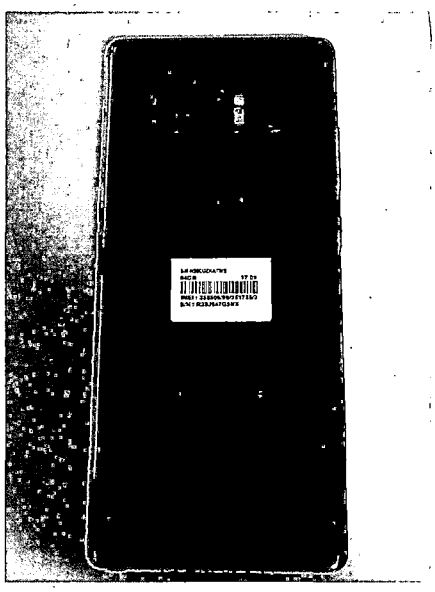
Hon. Peter E. Ormsby
UNITED STATES MAGISTRATE JUDGE

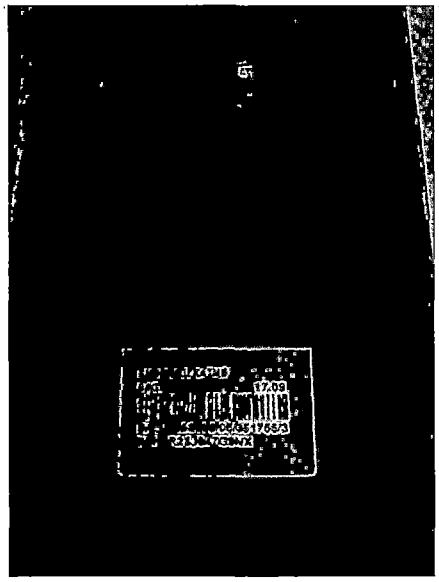
ATTACHMENT B

The property to be searched is:

1. Samsung cellular telephone, Model SM-N950U, IMEI: 358505083517553, S/N: R28J947G9NX, also referred to as "electronic device 1."







This device is currently in secure evidence storage at the HSI McAllen office located at 5901 S. International Parkway; McAllen, Texas 78503.

ATTACHMENT C

ITEMS TO BE SEIZED

1. All records on the device described in Attachment A that relate to violations of 21 U.S.C. § 841, 846 including:

   a. lists of co-conspirators and related identifying information;

   b. communications relating to the planning and carrying out of the controlled substances smuggling;

   c. types, amounts, and prices paid for controlled substances as well as dates, places, and amounts of specific transactions;

   d. any information related to the motivation for the controlled substances smuggling (including names, addresses, phone numbers, or any other identifying information of unidentified co-conspirators);

   e. any information related to the length and nature of the controlled substances smuggling;

   f. any information related to sources of controlled substances (including names, addresses, phone numbers, or any other identifying information);

   g. any information recording Hortencia Lerma's travel itinerary schedule or actual travel;

   h. any Global Positioning System technology information;

2. all bank records, checks, credit card bills, account information, and other financial records contained within the cellular device.

3. Evidence of user attribution showing who used and/or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

4. All evidence in support of illegal activity including violations of 21 U.S.C. § 841, 846.